UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,100	01/12/2001	W. David Shambroom	96-3-512CON1CIP2	1842

32127 7590 04/04/2006

VERIZON CORPORATE SERVICES GROUP INC.
C/O CHRISTIAN R. ANDERSEN
600 HIDDEN RIDGE DRIVE
MAILCODE HQE03H14
IRVING, TX 75038

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/04/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/759,100	SHAMBROOM, W. DAVID	
	Examiner	Art Unit	
	Kaveh Abrishamkar	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed on January 10, 2006.

2. Claims 1-36 are currently pending.

Response to Arguments

3. Applicant's arguments filed January 10, 2006 have been fully considered but they are not persuasive for the following reasons:

4. Regarding claims 1 and 23, the Applicant argues that the Cited Prior Art (CPA), Krajewski, Jr. et al. (U.S. Patent 5,590,199), does not teach "a network server." This argument is not found persuasive. The CPA teaches that the user workstation (client computer) and the authorization/authentication server are connected via a network (Figure 3). Furthermore, each secure computer service that the user accesses is connected via a network and users must prove their identity to these system services (column 5 lines 7-13). Therefore, it is asserted that a "network server" is disclosed in the CPA. Furthermore, the Applicant argues that the CPA does not teach "transmitting the message from the network server to the destination sever over the second secure connection." This argument is not found persuasive. The CPA discloses the client sending an authenticator and a server ticket (message) to the desired service (network server) where then the Server Kerberos (destination sever) decrypts the server ticket and authenticates the user (column 7 lines 20-24). Therefore, it is asserted that the

CPA does teach "transmitting the message from the network server to the destination sever over the second secure connection." Furthermore, the Applicant argues that the CPA does not teach a "gateway computer." However, in the present application, the gateway computer is analogous to the network server, and the arguments for the CPA teaching the network server can be applied to the gateway computer.

Therefore, the rejection for the claims is maintained below and applied to the amended limitations.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krajewski, Jr. et al. (U.S. Patent 5,590,199) in view of Fischer (U.S. Patent No. 5,005,200).

Regarding claim 1 Krajewski discloses:

A method of enhancing the security of a message sent by a principal from a client computer through a network server to a destination server.

Krajewski discloses "***obtaining by the client computer credentials for authorizing the principal from a validation center***" wherein the client requests a user id (credentials) form a Kerberos Authentication Server (validation center) (column 4 lines 66 – column 5 line 13, column 6 lines 40-47), "***transmitting from the client computer to the network server over the first connection the principal-authenticating credentials and the message***", wherein the KAS generates the user's ticket granting ticket and associated session key, encrypts the session key using the user's private key, and sends the message to the client (column 6 lines 47-51), and then the user sends the credentials to a system service (network server) (column 6 lines 58-64), "***transmitting the principal-authenticating credentials from the network server to the validation center***", wherein the KAS (validation server) validates the request (column 7 lines 5-10), "***transmitting permission data for the network server from the validation server to the network server based on the principal-authenticating credentials***" wherein the server (destination server) being accessed decrypts the ticket received from the KAS (validation server) and authenticates the user (column 7 lines 15-20), "***verifying the authorization of the principal in the network server***", wherein the server (destination server) being accessed decrypts the ticket received from the KAS (validation server) and authenticates the user (column 7 lines 15-20), and "***transmitting the message from the network server to the destination server over the second connection***" wherein the client sends an authenticator and a server ticket (message) to the Kerberos Server (destination server), (column 7 lines 15-25).

Krajewski does not explicitly disclose, "***establishing a secure connection for exchanging data between the client and the network server***" and "***establishing a second secure connection between the network server and the destination server***" or "***issuing a digital certificate to a network server***." However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 2 is rejected as applied above in rejecting claim 1. Krajewski does not explicitly disclose using SSL in establishing a secure connection. However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). It would have been obvious to use SSL to secure the connections between the servers and clients, as SSL provides a secure and repudiated connection between network entities.

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1, wherein the establishing step b further comprises the substeps of:

transmitting from the network server to the client server a network server key associated with a public-private key pair and a known cryptographic algorithm (column 7 lines 5-15);

transmitting from the client server to the network server a session key encrypted using the known cryptographic algorithm and the network server key (column 6 lines 48-52).

Krajewski does not explicitly disclose using SSL in establishing a secure connection. However, Fischer, in an analogous environment, discloses a trusted authority creating

and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27), wherein the cryptographic algorithm and the session key are used to set up an SSL session. It would have been obvious to use SSL to secure the connections between the servers and clients, as SSL provides a secure and repudiated connection between network entities.

Claim 4 is rejected as applied above in rejecting claim 1. Krajewski does not explicitly disclose using SSL in establishing a secure connection. However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). It would have been obvious to use SSL to secure the connections between the servers and clients, as SSL provides a secure and repudiated connection between network entities.

Claim 5 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1, wherein the establishing step (g) further comprises the substeps of:

transmitting from the destination server to the network server a destination server key associated with a public-private key pair and a known cryptographic algorithm (column 7 lines 5-15);

transmitting from the network server to the destination server a session key encrypted using the known cryptographic algorithm and the destination server key (column 6 lines 48-52); and

Krajewski does not explicitly disclose using SSL in establishing a secure connection. However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27), wherein the cryptographic algorithm and the session key are used to set up an SSL session. It would have been obvious to use SSL to secure the connections between the servers and clients, as SSL provides a secure and repudiated connection between network entities.

Claim 6 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1, wherein the obtaining step a further comprises the substeps of:

"***sending a request for credentials for the principal to the validation center***" wherein the client requests a user id (credentials) form a Kerberos Authentication Server (validation center) (column 4 lines 66 – column 5 line 13, column 6 lines 40-47);

"***receiving the credentials for the principal from the validation center***" wherein the client requests a user id (credentials) form a Kerberos Authentication Server (validation center) (column 4 lines 66 – column 5 line 13, column 6 lines 40-47); and

"***storing the credentials in the credentials cache on the client server***" (column 6 lines 50-57), wherein the session key is stored.

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1 wherein the principal-authenticating credentials comprises a ticket-granting ticket and a session key (Figure 5).

Claim 8 is rejected as applied above in rejecting claim 7. Furthermore, Krajewski discloses:

The method of claim 7 wherein the transmitting step (d) further comprises the substep of:

transmitting from the network server to the validating center a ticket-granting ticket and an authenticator (column 5 lines 25-39).

Claim 9 is rejected as applied above in rejecting claim 8. Furthermore, Krajewski discloses:

The method of claim 8 wherein the ticket-granting ticket comprises a session key encrypted with a permanent key for the validation center (column 5 lines 14-24).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Krajewski discloses:

The method of claim 9 wherein the authenticator is a data structure encrypted using the session key (column 5 lines 25-33).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Krajewski discloses:

The method of claim 10 wherein the transmitting step (e) further comprises the substep of:

decrypting the ticket-granting ticket at the validation center to extract a session key (column 7 lines 20-25).

Claim 12 is rejected as applied above in rejecting claim 11. Furthermore, Krajewski discloses:

The method of claim 11 wherein the permission data comprises an authenticator (column 7 lines 20-25).

Claim 13 is rejected as applied above in rejecting claim 12. Furthermore, Krajewski discloses:

The method of claim 12 wherein the authenticator comprises a data structure encrypted with the session key (column 7 lines 8-15).

Claim 14 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1 further comprising the steps of:

transmitting a request for a server ticket from the network server to the validation center (column 6 lines 43-50);

creating a server ticket for the network server at the validation center (column 6 lines 43-50); and

receiving the server ticket from the validation center at the network server (column 6 lines 51-55).

Claim 15 is rejected as applied above in rejecting claim 5. Krajewski does not explicitly disclose "extracting an access list and verifying that the principal is authorized to access a digital certificate and a destination server key" and "issuing a digital certificate and a destination server key." However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol

by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Fischer discloses "a digital certificate that conforms with the X.509 standard" (column 3 lines 53 – column 4 line 27).

Claim 17 is rejected as applied above in rejecting claim 1. Krajewski does not explicitly disclose "establishing a secure connection from the network server to more than one destination server." However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server),

which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Krajewski discloses:

The method of claim 17 wherein each connection between the network sever and a destination server is managed by a separate remote command execution client

(column 6 lines 55-64), wherein each separate requested service (destination server) uses a different ticket and a different session key.

Claim 19 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1 wherein the validation center utilizes a Kerberos protocol (column 5 lines 14-25).

Claim 20 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1 wherein the message comprises command data (column 6 lines 47-51).

Claim 21 is rejected as applied above in rejecting claim 20. Furthermore, Krajewski discloses:

The method of claim 20 wherein the command data comprise a remote user name, a destination server list and a command (column 6 lines 47-51).

Claim 22 is rejected as applied above in rejecting claim 1. Furthermore, Krajewski discloses:

The method of claim 1 further comprising the step of temporarily storing the principal-authenticating information (column 6 lines 50-57), wherein the session key is stored.

Regarding claim 23, Krajewski discloses:

A method of enhancing the security of a message sent by a principal from a client computer through a network server to a destination server.

Krajewski discloses "***obtaining by the client computer credentials for authorizing the principal from a validation center***" wherein the client requests a user id (credentials) form a Kerberos Authentication Server (validation center) (column 4 lines 66 – column 5 line 13, column 6 lines 40-47), "***transmitting from the client computer to the network server over the first connection the principal-authenticating credentials and the message***", wherein the KAS generates the user's ticket granting ticket and associated session key, encrypts the session key using the user's private key, and sends the message to the client (column 6 lines 47-51), and then the user sends the credentials to a system service (network server) (column 6 lines 58-64), "***transmitting the principal-authenticating credentials from the network server to the validation center***", wherein the KAS (validation server) validates the request (column 7 lines 5-10), "***transmitting permission data for the network server from the validation server to the network server based on the principal-authenticating credentials***" wherein the server (destination server) being accessed decrypts the ticket received from the KAS (validation server) and authenticates the user (column 7 lines

15-20), "***verifying the authorization of the principal in the network server***", wherein the server (destination server) being accessed decrypts the ticket received from the KAS (validation server) and authenticates the user (column 7 lines 15-20), and "***executing a command interpreter in the destination computer wherein the command interpreter may execute commands sent by the client computer***" wherein the client sends an authenticator and a server ticket (message) to the desired service (destination server) in order to access the desired service (column 7 lines 15-25).

Krajewski does not explicitly disclose, "***establishing a secure connection for exchanging data between the client and the network server***" or "***issuing a digital certificate to a network server.***" However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of

Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Regarding claim 24, Krajewski discloses:

A computer system for enhancing the security of one or more messages sent by a principal comprising:

"***a client computer for transmitting principal-authenticating credentials and the one or more messages***", wherein the KAS generates the user's ticket granting ticket and associated session key, encrypts the session key using the user's private key, and sends the message to the client (column 6 lines 47-51), and then the user sends the credentials to a system service (network server) (column 6 lines 58-64),;

"***a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials and the one or more messages from the client computer***" wherein the KAS generates the user's ticket granting ticket and associated session key, encrypts the session key using the user's private key, and sends the message to the client (column 6 lines 47-51), and then

the user sends the credentials to a system service (network server) (column 6 lines 58-64);

"***a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer***" wherein the server (destination server) being accessed decrypts the ticket received from the KAS (validation server) and authenticates the user (column 7 lines 15-20); and

"***one or more host computers operatively connected to the gateway computer and operating on any computer platform***" wherein the client sends an authenticator and a server ticket (message) to the desired service (destination server) in order to access the desired service (column 7 lines 15-25).

wherein the gateway computer transmits the one or more messages to at least one of the host computers wherein the client sends an authenticator and a server ticket (message) to the desired service (destination server) in order to access the desired service (column 7 lines 15-25).

Krajewski does not explicitly disclose, "***establishing a secure connection for exchanging data between the client and the network server.***" However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line

27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 25 is rejected as applied above in rejecting claim 24. Furthermore, Krajewski discloses:

The system of claim 24 wherein "***the gateway computer further comprises a gateway certificate server for transmitting the principal-authenticating credentials to the validation center and for receiving the permission data from the validation computer***" wherein the server (destination server) being accessed decrypts the ticket

received from the KAS (validation server) and authenticates the user (column 7 lines 15-20).

Claim 26 is rejected as applied above in rejecting claim 24. Krajewski does not explicitly disclose "establishing a secure connection to one or more host computers based on the permission data." However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in

future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 27 is rejected as applied above in rejecting claim 24. Krajewski does not explicitly disclose "establishing a secure connection to one or more host computers and the gateway computer based on the permission data." However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public

key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 28 is rejected as applied above in rejecting claim 27. Furthermore, Krajewski discloses:

The system of claim 27 wherein the host proxy and execution server executes a command interpreter for executing commands contained in the one or more messages wherein the client sends an authenticator and a server ticket (message) to the desired service (destination server) in order to access the desired service (column 7 lines 15-25).

Regarding claim 29, Krajewski discloses:

A computer system for providing a remote interactive login connection comprising:

"***a client computer for transmitting principal-authenticating credentials***", wherein the KAS generates the user's ticket granting ticket and associated session key, encrypts the session key using the user's private key, and sends the message to the client (column 6 lines 47-51), and then the user sends the credentials to a system service (network server) (column 6 lines 58-64),;

"***a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials***" wherein the KAS generates the user's ticket granting ticket and associated session key, encrypts the

session key using the user's private key, and sends the message to the client (column 6 lines 47-51), and then the user sends the credentials to a system service (network server) (column 6 lines 58-64);

"***a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer***" wherein the server (destination server) being accessed decrypts the ticket received from the KAS (validation server) and authenticates the user (column 7 lines 15-20); and

"***one or more host computers operatively connected to the gateway computer and operating on any computer platform***" wherein the client sends an authenticator and a server ticket (message) to the desired service (destination server) in order to access the desired service (column 7 lines 15-25).

Krajewski does not explicitly disclose, "***establishing a secure connection for exchanging data between the client and the network server.***" However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access

indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claims 30-31 are rejected as applied above in rejecting claim 29. Krajewski does not explicitly disclose "establishing a secure connection to one or more host computers and the gateway computer based on the permission data." However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access

indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Krajewski discloses:

The system of claim 31 wherein the host proxy and execution server executes a command interpreter for executing commands wherein the client sends an authenticator and a server ticket (message) to the desired service (destination server) in order to access the desired service (column 7 lines 15-25).

Claims 33-34 are rejected as applied above in rejecting claim 29. Krajewski does not explicitly disclose "using a downloadable executable interactive client (DEIC) comprising

a Java applet for establishing a secure connection with the gateway computer." However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Claim 35 is rejected as applied above in rejecting claim 29. Furthermore, Krajewski discloses:

The system of claim 29 wherein the gateway computer temporarily stores the principal-authenticating information (column 6 lines 50-57), wherein the session key is stored.

Regarding claim 36 Krajewski discloses:

A computer program product for use with a computer system, the compute program product comprising a computer readable storage medium and a computer program stored therein for carrying out a process.

Krajewski discloses "***obtaining by the client computer credentials for authorizing the principal from a validation center***" wherein the client requests a user id (credentials) form a Kerberos Authentication Server (validation center) (column 4 lines 66 – column 5 line 13, column 6 lines 40-47), "***transmitting from the client computer to the network server the principal-authenticating credentials and the message***", wherein the KAS generates the user's ticket granting ticket and associated session key, encrypts the session key using the user's private key, and sends the message to the client (column 6 lines 47-51), and then the user sends the credentials to a system service (network server) (column 6 lines 58-64), "***transmitting the principal-authenticating credentials from the network server to the validation center***", wherein the KAS (validation server) validates the request (column 7 lines 5-10), "***transmitting permission data for the network server from the validation server to the network server based on the principal-authenticating credentials***" wherein the server (destination server) being accessed decrypts the ticket received from the KAS

(validation server) and authenticates the user (column 7 lines 15-20), "***verifying the authorization of the principal in the network server***", wherein the server (destination server) being accessed decrypts the ticket received from the KAS (validation server) and authenticates the user (column 7 lines 15-20), and "***transmitting the message to the destination server***" wherein the client sends an authenticator and a server ticket (message) to the desired service (destination server), (column 7 lines 15-25).

Krajewski does not explicitly disclose, "***establishing a secure connection for exchanging data between the client and the network server***" or "***issuing a digital certificate to a network server.***" However, Fischer, in an analogous environment, discloses a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL) (column 3 line 53 – column 4 line 27). U.S. Patent No. 5,923,756 discloses in claim 14 "authenticating that the party transmitting the message to said destination server is the same party that was certified using the authentication protocol by the key distribution center to receive said access indicator." The "authenticating" step does not explicitly state via a digital certificate, but digital certificates were well known in the art at the time the Applicant's invention was made as disclosed by Fischer. Therefore, it would have been obvious to one of ordinary skill in the art at the time the Applicant's invention was made to incorporate the teachings of Fischer into the system Krajewski to provide a method of verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital

certificate to the network server before establishing a secure connection. This modification would have been obvious because one of ordinary skill in the art would want to use a digital certificate to not only provide non-repudiation between the network server and the destination server, but also, to provide the public key that will be used in future secure communications simultaneously to conserve network resources while increasing the overall security of the network.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kaveh Abrishamkar whose telephone number is 571-272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

KA
03/31/2006

CHRISTOPHER REVAK
PRIMARY EXAMINER

3/31/06